



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

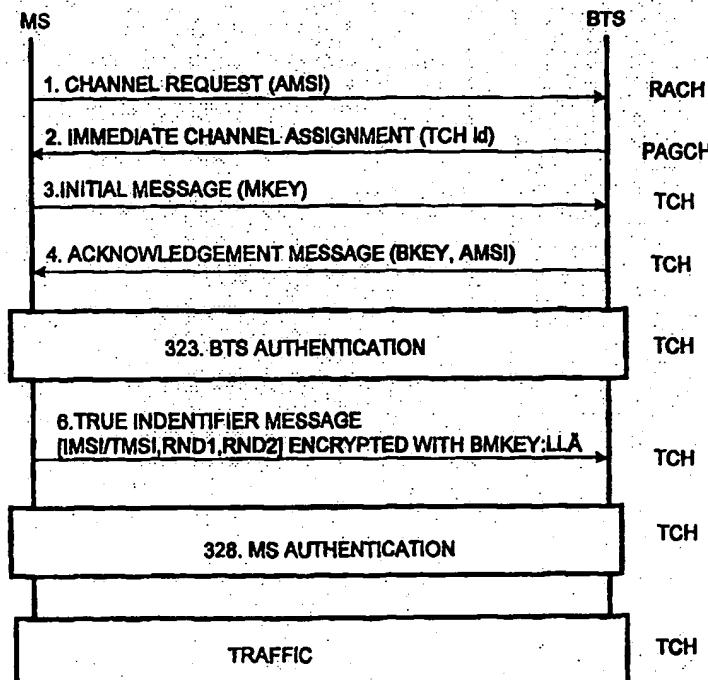
(51) International Patent Classification ⁶ :	A1	(11) International Publication Number: WO 98/26538
H04L 9/32, H04Q 7/38		(43) International Publication Date: 18 June 1998 (18.06.98)

(21) International Application Number: PCT/FI97/00765	(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).
(22) International Filing Date: 8 December 1997 (08.12.97)	
(30) Priority Data: 964926 10 December 1996 (10.12.96) FI	
(71) Applicant (for all designated States except US): NOKIA TELECOMMUNICATIONS OY [FI/FI], Keilalahdentie 4, FIN-02150 Espoo (FI).	
(72) Inventor; and	Published
(75) Inventor/Applicant (for US only): JUOPPERI, Jari [FI/FI]; Luutnantintie 3 D 30, FIN-00410 Helsinki (FI).	With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments. In English translation (filed in Finnish).
(74) Agent: PATENT AGENCY COMPATENT LTD.; Teollisuuskatu 33, P.O. Box 156, FIN-00511 Helsinki (FI).	

(54) Title: AUTHENTICATION BETWEEN COMMUNICATING PARTIES IN A TELECOMMUNICATIONS NETWORK

(57) Abstract

In known telecommunications systems using multiple access the terminal equipment assumes that the network element is genuine while the network element assumes that the terminal equipment is genuine. This allows false terminal equipment, a false network element or a third party to penetrate the system. The proposed commitment protocol applies bit block commitment known from cryptography and a shared encryption key and the authentication is divided into two parts, whereby one part of it is done by the terminal equipment and the other part is done by the network. The terminal equipment (MS) sends to the network element (BTS) a pseudo identifier (AMSI) which it has formed, whereupon encryption keys (MKEY, BKEY) are exchanged. Only when the network element has revealed its true identity, will the terminal equipment send the required information (IMSI, RND₁, RND₂) encrypted with a combination of the keys. Finally, the network element authenticates the terminal equipment by using the identity information which it has revealed. Only then can operation commence.



Best Available Copy

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

Authentication between communicating parties in a telecommunications network

Field of the invention

5 This invention concerns origination of data transmission in a multiple access network, wherein the terminal equipment requests a channel for itself from the network using a common access channel intended for all terminal equipment and wherein in response to the request the network on a common access grant channel intended for all terminal equipment makes known that channel to the terminal equipment on which information transmission proper will take place.

Background of the invention

15 It is a general principle in telecommunications networks using multiple access that for using services of the network the terminal equipment by using some uplink access method must first inform the network of its desire to gain access to the network. This takes place so that e.g. a special channel is reserved in the network as a common channel for all terminal equipment, which send a request on this channel to obtain a service.

20 Depending on the network, this request may contain just a request to have a channel for two-way data transmission or it may contain information on which particular service is desired and possibly also information on the desired channel capacity. The channel may be a stream type or packet channel. The layer relaying requests is called the Medium Access Control Sublayer (MAC layer) according to the OSI model and it uses services of the physical layer to produce services for the control layer of the logical link.

30 In time-division cellular multiple access networks a channel is assigned on which all mobile stations when forming mobile originated calls send a request for a traffic channel from the network. The request, which is relayed over the radio path to the base station and from this along a cable to the base station controller, contains the mobile station's identifier IMSI, so that the base station controller will know from whom the request has come. In a GSM system such a channel used by all is called Random Access Channel (RACH). Should collisions between requests occur on the channel, the mobile station will try again after a moment until the request is received. The network sends to the mobile stations acknowledgements of the requests

on a channel to which all mobile stations are listening. In a GSM system this channel is called Access Grant Channel (AGCH): the acknowledgement contains the mobile station's identifier, from which the mobile station will know that the message is intended for itself, and the number of the channel allocated by the network as a traffic channel.

Access in accordance with the MAC protocol is also used in interactive cable TV systems, where a desired audiovisual service can be transferred to several recipients through a fixed network. The physical transfer path may be a coaxial cable and/or an optical cable or a radio network or the distribution may take place through a satellite. In the system the name Head End is given to a central place where an incoming dispatch is divided over several physical signal paths, such as several optical fibers, by which the dispatch is taken closer to the consumers. In the systems, transmission may take place both in downlink and uplink directions in time slots which are numbered starting from zero and ending with some max number, after which numbering starts again. The time slots 0,..., max form a frame. For terminals to be able to send information upwards, such a channel may be used in the uplink direction where the access form is Aloha, whereby all subscribers may send requests in any time slot. The network acknowledges a successful transmission by echo checking on a downlink channel. In the uplink direction, only a certain time slot may alternatively be used for sending requests. This is a slotted Aloha access type. It is essential also in these systems for the terminal to include its identifiers in its access message, so that the Head End may know who sent the request.

It is characteristic according to Figure 1 for systems of the described type that when several terminal equipment A wish to communicate with network B, they request a private channel on a common channel U. The request message contains requestor A's identifier. The network element may perform authentication of the requestor, and if the matter is OK, it will allocate a private channel T for the requestor and will send information about the channel either on the same common channel U or on another common return path channel D. The information contains requestor A's identifier. A receives the message and begins communicating on the allocated channel T.

Figure 2 shows exchange of messages used in network access in a known GSM mobile telephone system. When a mobile station wishes to

form a call, it sends on a one-way (uplink direction) Random Access Channel (RACH) to the base station a Channel Request to have a Traffic Channel (TCH) at its disposal, step 211. The request contains a 5-bit random number, which first functions as the mobile station's identifier. The base station receives, step 213, and relays the request to the base station controller, which selects a free channel, activates it on the base station, step 212, and then forms an Immediate Assignment, which the base station sends on a Paging and Access Grant Channel (PAGCH) to the mobile station, step 214. The assignment contains a description of the allocated channel, a preset timing value, the transmission power value to be used and the same 5-bit random number which was sent by the mobile station, and also the time slot number with which the base station had received the channel request. With this information the mobile station is able to distinguish the message intended for itself and will learn the allocated traffic channel, step 215.

15 The mobile station then signals to the base station on the traffic channel the link layer initial message containing the SABM frame. In this message the mobile station states its identity IMSI (International Mobile Subscriber Identity) or its Temporary Mobile Subscriber Identity (TMSI), step 224. The base station receives the message, step 226, and acknowledges it with a response message, the UA frame of which contains the identity of the mobile station, step 228. The mobile station compares its own identity with the received identity, step 223, and if the identities are similar, it will know that the traffic channel is reserved for itself.

20 Before starting operation, authentication is also performed on the principle that the network puts a question to the mobile station to which only the right mobile station will know the answer. Authentication is based on an authentication algorithm A3 and on a subscriber-specific authentication key K_s . In the early part of authentication the authentication center AuC sends a question to the mobile station which is a random number RAND. The mobile station receives the RAND, transfers it to the SIM card, which performs the A3 algorithm with its aid and with the aid of the subscriber-specific key K_s in the card. The Signed Result (SRES) is sent by the mobile station to the network. Authentication center AuC compares the SRES value with the value which it has computed itself using the same A3 algorithm, RAND and key K_s . 25 If the SRESs are identical, the authentication is approved, otherwise the subscriber is denied access to the network. The mobile station uses the

received RAND and K_i values also for computing a connection-specific encryption key K_c . In the network, authentication center AuC performs the same algorithm with the same values, thus resulting in the same encryption key. Both store the key in memory and in addition the mobile station sends the key to authentication center AuC, which checks to make sure that both are using the same keys.

It is a noteworthy feature in the process shown in Figure 2 that the mobile station has sent its own identity to the network before it is quite sure that the traffic channel is allocated to itself and to nobody else.

10 It is taken for granted in known systems of the type shown in Figure 1 that the party A requesting access knows as a matter of course that network element B is exactly what A assumes it to be and that network element B will not doubt that the terminal equipment using the received symbol is terminal equipment A.

15 It is a problem in these systems that the network always performs the authentication. It is hereby possible for a third party to come between the identifying party and the one to be identified, to eavesdrop on the first messages and to put himself in the other party's place. This is possible especially if a part of the transmission path between A and B is a radio path, 20 which is the case in mobile telephone networks, but likewise in fixed networks a third party may connect to the line and eavesdrop on the traffic. It is hereby possible for the third party to capture a channel request message sent by terminal equipment A and to interpret from this the request and, above all, A's identifier. It will then in one way or another eliminate terminal equipment A and take its place. It then receives the channel allocation message sent by the network element, connects to the channel pretending to be terminal equipment A and thus gains access to the network. There is no possibility for network element B to know that it is communicating with a third party instead of the genuine terminal equipment A.

30 It is also possible for network element B to be the impostor. Hereby terminal equipment A when contacting network element B immediately gives it its identity data in the first message. B hereby knows who A is, but A does not know that B is only pretending to be A. Such a situation is possible e.g. in mobile station networks, whereby a "false" base station may take the place of the genuine one and thus eavesdrop on and 35 control the radio traffic.

It is not possible with state-of-the-art systems to prevent situations as those described above. The present invention thus aims at a method by which it is possible to prevent the described situations, and such a case in particular where the terminal equipment never discloses its identity to any

5 third party eavesdropping on the traffic between the terminal equipment and the network element and where the terminal equipment will disclose its identity only when being sure that the network element really is the one it declares itself to be, whereby when the network element is an impostor it will never know the true identity of the terminal equipment.

10 The method according to the invention is characterized by the features defined in the independent claims.

Brief summary of the invention

The proposed method is based on the fact that the commitment protocol applies bit commitment known from cryptography and a shared encryption key and that authentication is divided into two, whereby a part of the authentication is done by the terminal equipment and the other part is done by the network. The terminal equipment first makes sure that the network element is authentic by performing authentication of the network element. In this connection the network element will disclose its own identity. Then the terminal equipment reveals its own identity to the network element by sending the necessary information on a protected channel. Finally, the network element authenticates the terminal equipment by using the identity information which it has disclosed. Only after this can traffic be started.

25 The terminal equipment requesting access in the commitment protocol first makes a pseudo identifier for itself, which it forms by applying a one-way hash function to its correct identifier. The hash function is not applied to the identifier as such, but the correct identifier is first encrypted. This being the case, the network or network element upon receiving the pseudo identifier can not get to know the correct identifier without the code. When the network element has stated the traffic channel to the terminal equipment, about which it knows only the pseudo identifier at this stage, the terminal equipment will generate its own security key half, that is, the first partial key, and will send it to the network. On receiving the partial key the

30 network element will also form its own security key half, that is, the second

35

partial key. It sends these to the terminal equipment of the pseudo identifier, so both parties will at this stage have both partial keys in their possession.

The terminal equipment checks if the pseudo identifier received from the network element and the pseudo identifier it formed earlier itself are identical, and if they are, it will perform authentication of the network element in some known manner.

After authentication, the network element has revealed itself to the terminal equipment, but the real identity of the terminal equipment is still known only to the terminal equipment. The network element will not get to know the real identity until the terminal equipment has sent information to it on how the true identity was encrypted before the use of the hash function.

The terminal equipment now send its own true identifier to the network element. For this purpose, the terminal equipment forms a message containing a) its true identifier, b) information on how the true identifier was encrypted before application of the hash function. It encrypts the message before sending it by using a key formed both of the first and of the second partial key.

The network element receives the message, decodes it using the first and second partial key and checks if the contents of the message are correct. If they are, the network element will perform authentication of the terminal equipment by some known method.

After a successfully performed commitment protocol and mutual authentication, traffic can be started on the traffic channel.

25

List of figures

The invention will be described in greater detail referring to the enclosed diagrammatic drawings, wherein

30 Figure 1 shows state-of-the-art message exchange;
Figure 2 shows message exchange in a mobile telephone system;
Figure 3 shows a commitment protocol according to the invention; and
Figure 4 illustrates exchange of messages.

35

Description of the invention in detail

Figure 3 shows a method according to the invention as applied to a GSM cellular system. It thus contains the same elements as the basic

procedure shown in Figure 2, so the description will also refer to Figure 2 when required.

The commitment protocol to be used in the invention requires five steps, each one of which is known from cryptography:

- 5 1. bit block commitment,
- 10 2. exchange of keys,
- 15 3. identification of the network element,
- 20 4. revealing the terminal equipment's identity to the network element, and
- 25 5. identification of the terminal equipment.

The method of bit block commitment is described in detail in a book by Bruce Schneier: "Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc, 1996, ISBN 0-471-11709-9. The method is such that

- 15 1) party A first forms random bit strings R1 and R2.
- 20 2) Then it forms a message containing these random bit strings and that bit string S (e.g. an identifier, some message or other), which it wishes to give to party B, however, so that party B will not get to know bit string S without A's permission. Random bit strings R1 and R2 as well as identifier S are simply located one after the other in the message.
- 25 3) Party A applies a one-way hash function h to the message and sends the result $h(R1, R2, S)$ and either one of the random strings, e.g. R1, to party B. This transmission proves to B that A has really sent bit string S. The use of a one-way hash function prevents B from inverting the function, and for this reason B, although knowing the hash function and one random string R1, can not get to know bit string S, because the other random string R2 is hashed.
- 30 4) When it is time for party A to disclose bit string S, it will send the original message (R1, R2, S) to party B.
- 35 5) Party B applies a one-way hash function to this message and compares the result and random string R1 to that which party A already sent earlier in step 3. If all tally, the received string S is correct.

In this known method, party B does not send even the first message. It is a known property of the one-way hash function that from a binary string of arbitrary length it will produce a string of a fixed length, "a secure fingerprint". Hereby, when $H=h(M)$, wherein M is a binary string of

arbitrary length, h is a one-way hash function and H is a binary string of fixed length, the following will hold: a) when M is given, H may be easily calculated, b) when H is given, it is impossible to find such an M that $h(M)=H$ would be true, c) when M is given, it is impossible to find such an M' that 5 $h(M')=h(M)$ would be true, and d) it is impossible to find two random strings M and M' so that $h(M)=h(M')$ would be true.

Of known hash functions which may be used in this invention, SHA (Secure Hash Algorithm) and MD5 (Message Digest Algorithm 5) may be mentioned, but it is of course possible in principle to use any kind of other 10 known hash function.

The purpose of the key exchange algorithm used in the commitment protocol is to form an encryption key for two or more parties even if there is no secure transfer channel between the parties. The Diffie-Hellman key exchange described in the publication referred to above and the RSA 15 public key encryption algorithm are well suited for use in this invention.

The commitment protocol according to the invention will now be described referring to Figure 3. Instead of sending only a random number in the channel request message on the call channel, the mobile station sends a pseudo identifier AMSI. This it forms as follows by using the one-way hash 20 function, step 311, Figure 3,

$$\text{AMSI} = h(\text{IMSI}, \text{RND}_1, \text{RND}_2)$$

wherein h is some one-way hash function, IMSI is the mobile station's real identifier, the first random number RND_1 is a string of binary figures of finite length while the second random number RND_2 is a string of 25 binary figures of finite length. Thus, the real identifier is coded in a sense with the first and second random numbers by simply placing the numbers and the identifier in a sequence to form a chain, and the hash function is applied to the chain. The mobile station sends its pseudo identifier AMSI and the first random number RND_1 through the transmission network to the 30 network element, step 312.

It should be noted that the transmission network may be either just a radio path or a combination of radio path and cable network depending on whether the network element means a base station, a base station controller or a mobile telephone exchange. The essential nature of the network element is not essential to the invention.

The base station controller receives relayed by the base station a channel request message containing a pseudo identifier AMSI, step 313, whereupon it performs selection and activation of the traffic channel, as in the known method, that is, step 23 in Figure 2, and in the normal manner 5 sends a channel allocation message, wherein the allocated traffic channel is indicated, step 314.

Then some transactions are performed in the commitment protocol before the real identifier IMSI is revealed. The mobile station first makes its own security key MKEY, which is here called the first partial key, 10 step 315. Information contained in the first partial key is used in the key exchange procedure to be carried out later. It places the partial key which it has formed in the originating message and it signals the message to the base station on the indicated traffic channel, step 316.

The network element receives the first partial key of the message, 15 step 317. It then makes its own security key BKEY, which is here called the second partial key, step 318. Information contained in the second partial key is used in the key exchange procedure to be performed later. It then forms an acknowledgement message containing the pseudo identifier AMSI which it received earlier and the second encryption key BKEY which it has formed, 20 and it sends an acknowledgement message to the mobile station, step 320.

The mobile station receives the acknowledgement message, step 321, and separates the elements of its contents. It examines first whether the pseudo identifier AMSI contained in the message is the same as the pseudo identifier AMSI which it created itself in step 311. If the comparison, 25 step 322, shows that the pseudo identifiers are different, the mobile station will know that the traffic channel indicated in step 314 was not intended for itself, so it must start the access process from the beginning, from step 311. If the comparison shows that the pseudo identifiers are identical, the mobile station will know that the traffic channel indicated in step 314 is really intended for 30 itself.

In the following step 323, the mobile station performs authentication of the network element to make sure that the network element, in this case a base station, really is what it claims to be. The authentication procedure may be any procedure, e.g. the authentication procedure 35 nowadays used in the GSM system is suitable.

After a successful authentication the mobile station knows that it is dealing with a real base station and not with an impostor, so it is time for it to reveal its true identity. To this end it forms a message containing the real identifier IMSI (or the temporary identifier TMSI, if there is one), the first random number RND, and the second random number RND₂. Thus, the message is the same as the one to which it applied the hash function in step 311. Finally, it encrypts the whole message with encryption key BMKEY, which is formed of the first partial key MKEY and of the second partial key BKEY, step 324. The mobile station sends this key-encrypted message to the network, step 325.

Now then, it is time for the network element to see which is the mobile station's true identifier. First, step 326, the network element decodes the encrypted message by using security key BMKEY, which is a combination of the second partial key BKEY which it generated itself in step 318 and of the first partial key MKEY received from the mobile station in step 317. The network element then performs a check of the validity of elements contained in the message, step 327. First, it calculates the result of the formula $AMSI = h(IMS1; RND1, RND2)$ calculated by using elements of the message. It then examines whether the AMSI produced by the formula is the same as the one it received earlier from the mobile station in step 313. Finally, it checks if the second random number RND, given in the message is the same as the one it received in step 313. If all AMSIs are exactly identical and the second random numbers tally, the network element will be assured that the mobile station is exactly the same as the one at issue in the beginning of the process. If the received values do not tally fully in the check, the network element will interrupt the access protocol and will remove the traffic channel from use by this session, whereby it may be allocated to some other connection.

If all things are okay so far, the network element will also perform authentication of the mobile station. If the authentication gives a proper result, traffic may commence on the indicated traffic channel.

The signal diagram in Figure 4 shows messages which are exchanged on the radio path between mobile station MS and base station BTS in the procedure shown in Figure 3. Excepting authentication messages, there is hardly any more exchange of messages in the proposed method than in a state-of-the-art GSM system. The main information

exchanged in the messages is shown within parentheses in the figure. The channels are also marked, and as can be noticed a major part of the messages is signaled on the traffic channel.

The purpose of the authentication of the network element, e.g. the 5 base station, in steps 323 in Figures 3 and 4 is to provide the terminal equipment, e.g. the mobile station, with a possibility to check that it shares the secret key MBKEY with an honest network element, in other words, that the network element has such an operator's certificate which the terminal equipment trusts. Authentication of the network element is limited by the 10 circumstance that the terminal equipment must perform authentication based on that information only which the network element supplies. ISO standard X.509 presents a set of authentication protocols which are suitable for use in this method. A brief description will be given of a straightforward protocol based on certificate and digital signature, as an example of a possible 15 protocol by which the mobile station may make sure the relation of the base station and the key MBKEY:

1. MS sends a randomly chosen string of binary figures RDN_3 to the base station.
2. The base station receives the RDN_3 and makes a message 20 containing a certificate and the RDN_3 . It signs the message with a digital signature and then encrypts the message by using the key MBKEY and sends the message to the mobile station.
3. The mobile station decodes the encrypted message, checks the 25 signature, the signature to the certificate and makes sure that the string of random figures sent in the message is the same as the one which it has sent earlier to the base station. If the message passes all these checks, then the authentication has given a positive result.

The purpose of the authentication of terminal equipment, e.g. of a 30 mobile station, by the network element in step 328 shown in Figures 3 and 4 is to give an honest network element a possibility to make sure that it shares a common secret key (MBKEY) with such a piece of terminal equipment, the identifier of which (IMSI/TMSI) is exactly the one which the terminal equipment has sent in its message revealing the true identifier in step 325 of 35 Figure 3. The authentication differs from the authentication performed by the terminal equipment (the mobile station) for the reason that the terminal equipment has already revealed its true identity. For this reason, the network

element performs an inquiry to some suitable database of the network asking for information about the terminal equipment which has this very identifier (IMSI/TMSI). In a mobile network the database is by nature a home location register (HLR). If the register information relating to the identifier indicates 5 that all is okay, then the authentication has given a positive result and traffic may commence.

When using a commitment protocol according to the invention, at least three security factors will be achieved:

Firstly, it is impossible for a third party to find out the identifier of 10 the terminal equipment when performing the protocol. It can be seen from Figure 4 that the identifier of the terminal equipment is sent in messages 1, 4 and 6. It results from the characteristics of the hash function described on page 7 that any trespasser can not possible calculate the true identifier from messages 1 and 4. The true identifier to be transmitted in step 6 is encrypted 15 with a common key, which is known only to the parties, so any trespasser can not find out the identifier without breaking the encryption algorithm.

Secondly, any foreign base station trying to put itself in the 20 position of the real base station may indeed capture messages 1-4, Figure 4, but if the authentication of the base station performed by the terminal equipment proceeds as it should, it will realize that the base station is not genuine and will discontinue the protocol. As the terminal equipment has sent its pseudo identifier only, no deceitful base station will be able in any 25 way to calculate the true identifier thanks to the characteristic of the one-way hash function.

Thirdly, an honest base station is able to conclude whether the 30 terminal equipment for which the channel was allocated is that very terminal equipment which sent the channel request. Based on the characteristics of the one-way hash function presented on page 7 it is impossible for any other terminal equipment than the one which has sent the channel request to calculate such parameters that would lead to an acceptable final result after 35 the reception of message 6 in the base station of Figure 4. Under these circumstances, the terminal equipment may on good grounds conclude if the traffic channel is intended exactly for itself, having received the acknowledgement message, message 4 in the figure.

The network element notices the attempt of a foreign terminal equipment to "steal" a traffic channel from the original requestor, step 6 in

Figure 4, because it has received the pseudo identifier AMSI from the requestor in the beginning of the protocol and because it is impossible for any foreign terminal equipment to calculate the second random number and the true identifier from the pseudo identifier.

5 The proposed commitment protocol adds to the traffic on the transmission path to some extent, mainly for the reason that message lengths will grow compared e.g. to typical message lengths in a GSM system. The length of the pseudo identifier is 160 bits, if the MD5 algorithm is used as hash function. If the Diffie-Hellman key exchange algorithm is
10 used in the key exchange, the amount of information to be transmitted will be at least 500-1000 bits.

15 The proposed commitment protocol may be applied within the scope of the claims to any telecommunications network where the terminal equipment using joint resources first requests a connection from the network for transmission of information and the network in response to the request indicates the required connection.

Claims

1. Method of authentication between communicating parties in a telecommunications network, wherein a network element and terminal equipment perform authentication of each other and wherein the network element in response to an access message of the terminal equipment allocates a traffic channel on which the traffic is carried out, characterized in that before traffic is started:
 - the terminal equipment sends such a pseudo identifier in the access message which contains its true identifier (IMSI) encrypted in such a way that the network element is able to find out the true identifier only after having received from the terminal equipment a new message, the content elements of which contain the true identifier non-encrypted,
 - the terminal equipment and the network element each form their own partial key and reveal these to each other on the traffic channel,
 - the terminal equipment performs authentication of the network element,
 - if the network element is found to be genuine, the terminal equipment forms a new message containing the true identifier non-encrypted and sends to the network element on the traffic channel a new message encrypted with both partial keys.
2. Method as defined in claim 1, characterized in that the terminal equipment forms a pseudo identifier (AMSI) by applying a one-way hash function to content elements comprising its true identifier (IMSI) and two random numbers (RND_1 , RND_2) and it sends the pseudo identifier (AMSI) and one of the random numbers (e.g. RND_1) in the access message.
3. Method as defined in claim 2, characterized in that the terminal equipment forms a first partial key (MKEY) and it sends this to the network element on the traffic channel,
- 30 the network element forms a second partial key (BKEY) and it sends this and the pseudo identifier (AMSI) to the terminal equipment on the traffic channel.
4. Method as defined in claim 3, characterized in that when the pseudo identifier received by the terminal equipment and the pseudo identifier which it formed earlier are identical, the terminal equipment will perform authentication of the network element.

5. Method as defined in claim 4, characterized in that after a successful authentication the terminal equipment will form a new message containing content elements of the hash function and will send the new message to the network element encrypted with the first and second partial keys.
6. Method as defined in claim 5, characterized in that the network element deciphers the encryption of the new message using the first and second partial keys and performs authentication of the content elements.
- 10 7. Method as defined in claim 6, characterized in that in the authentication the network element:
 - applies a hash function to the content elements and compares the result with that pseudo identifier (AMSI) which it has received earlier in the access message,
 - 15 it compares to find out whether the second random number (e.g. RND₂) stated in the message is identical to the one which it received earlier in the access message.
 - 20 8. Method as defined in claim 7, characterized in that when comparisons show that the pseudo identifier and the second random number are true, the network element will perform authentication of the terminal equipment.
 9. Method as defined in claim 1, characterized in that a cryptographic bit block commitment method known as such is used when forming the pseudo identifier and when stating the true identifier.
 - 25 10. Method as defined in claim 1, characterized in that Diffie-Hellman key exchanges known as such and RSA public key encryption algorithms are applied to the use of partial keys.

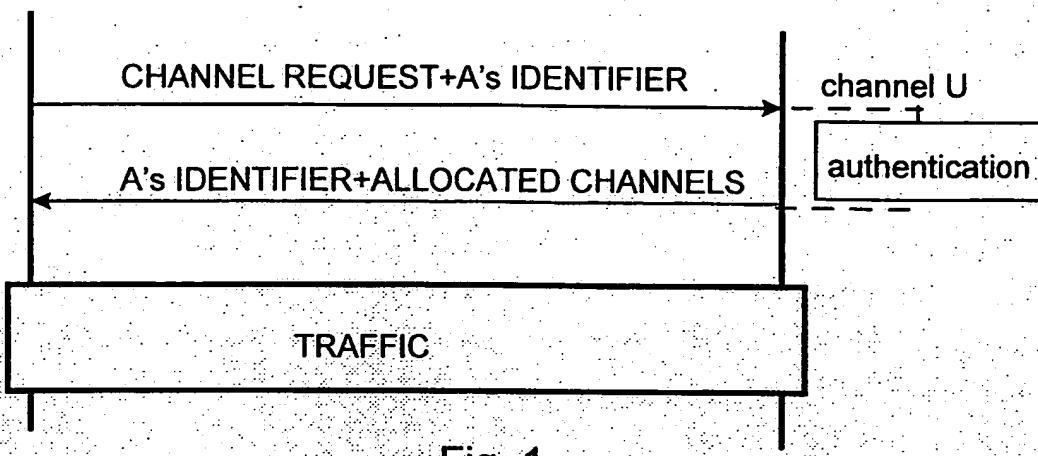


Fig. 1

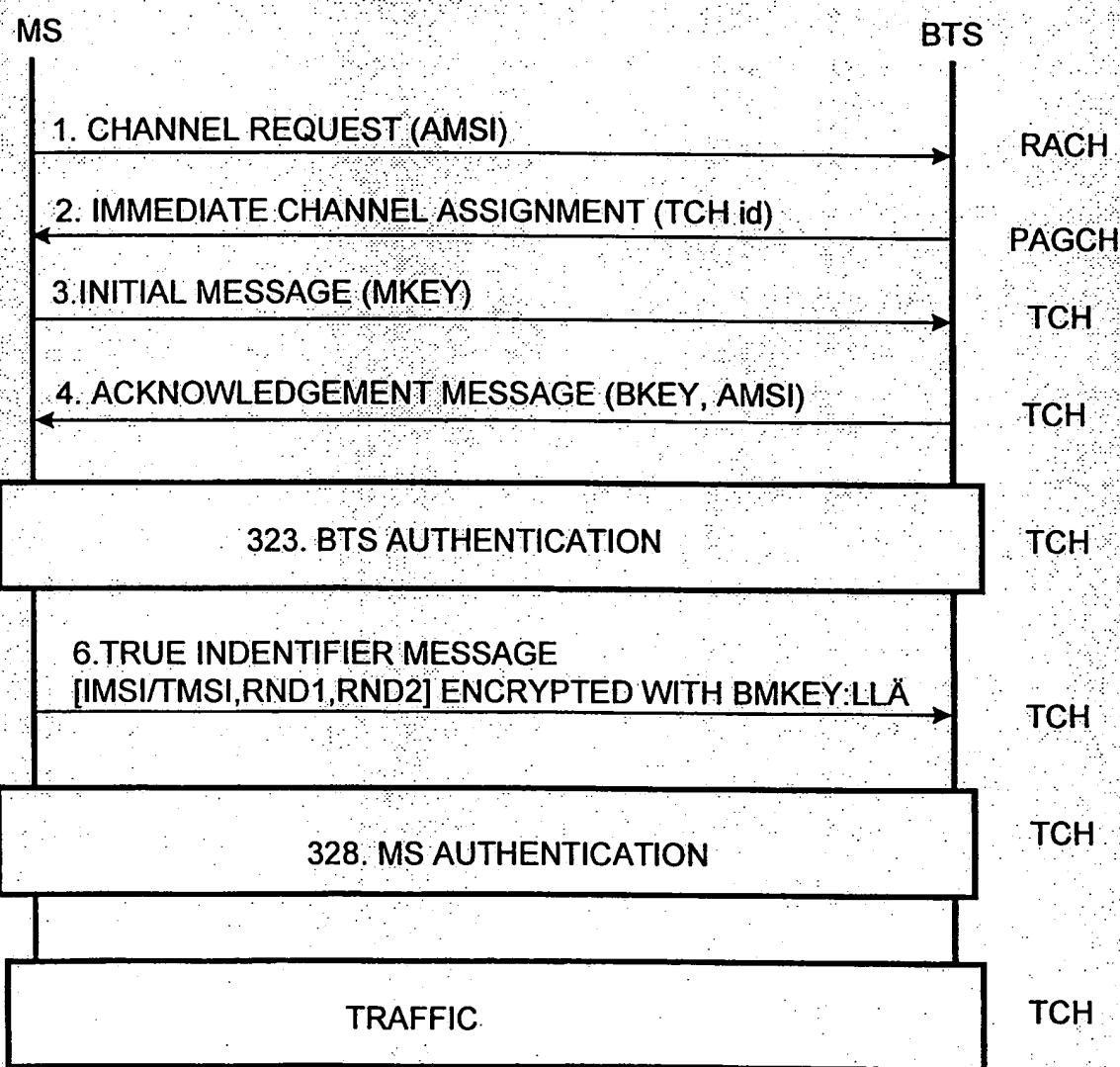


FIG. 4

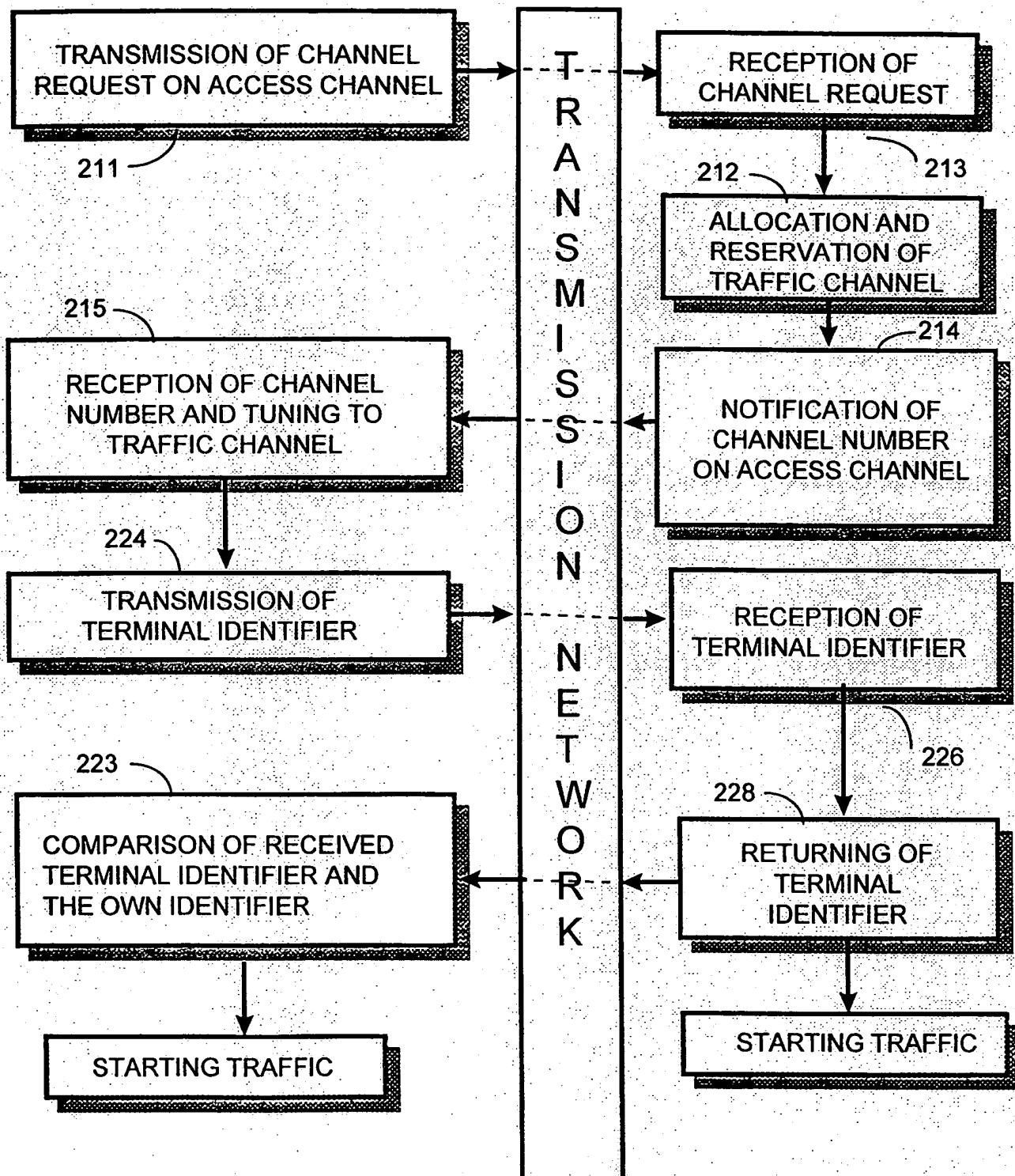


Fig. 2

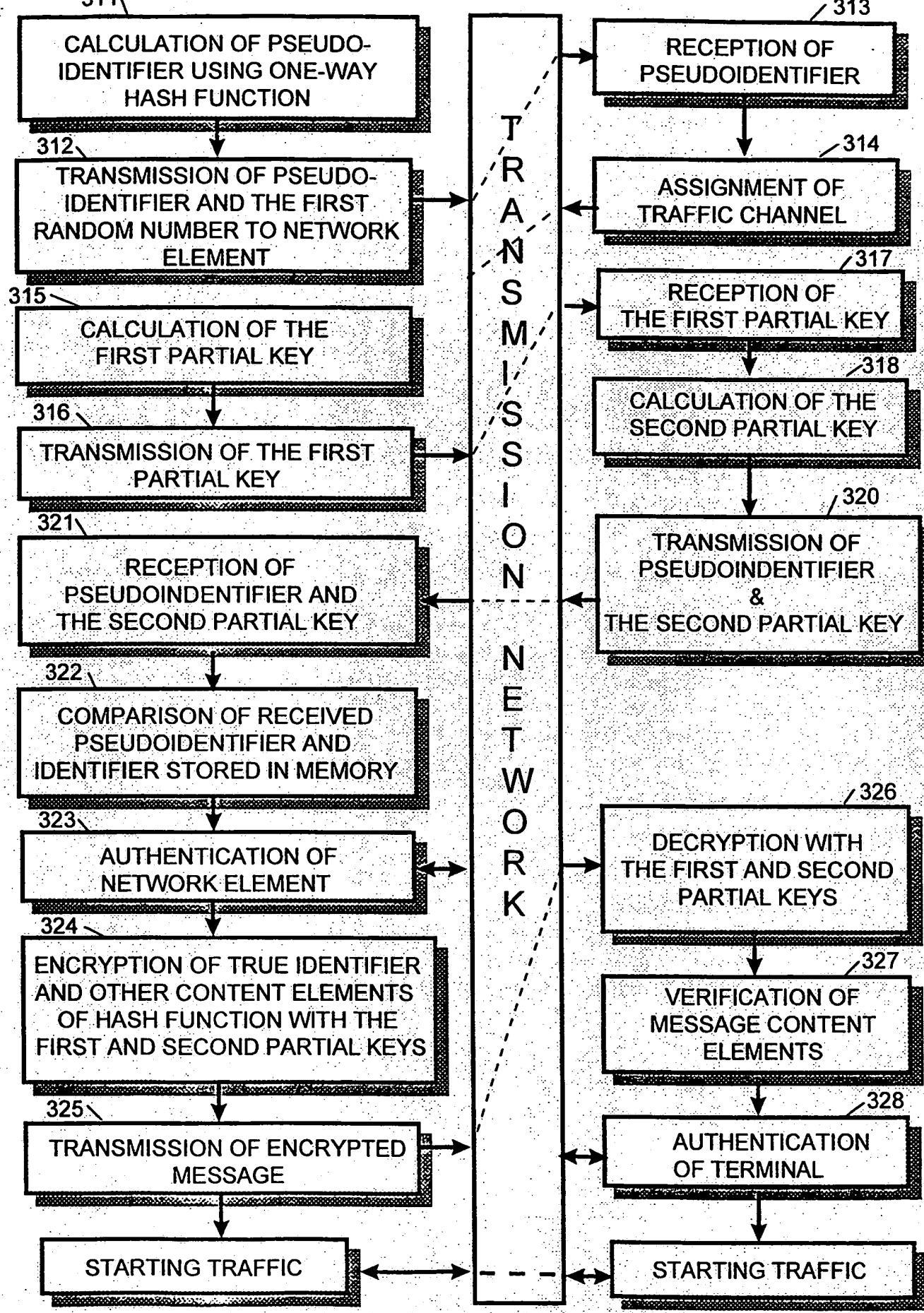


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 97/00765

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32, H04Q 7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0651533 A2 (SUN MICROSYSTEMS, INC.), 3 May 1995 (03.05.95), abstract	1-10
A	EP 0447380 B1 (TELEFONAKTIEBOLAGET LM ERICSSON), 18 Sept 1991 (18.09.91), column 2, line 9 - line 18	1-10
A	WO 9114348 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 19 Sept 1991 (19.09.91), page 4, line 18 - page 5, line 16	1-10

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

6 May 1998

Date of mailing of the international search report

07-05- 1998

Name and mailing address of the ISA/
Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. +46 8 666 02 86Authorized officer
Bengt Romedahl
Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 97/00765

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5345506 A (HIDEKI TSUBAKIYAMA ET AL), 6 Sept 1994 (06.09.94), column 2, line 57 – column 3, line 2	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

02/04/98

International application No.

PCT/FI 97/00765

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 0651533 A2	03/05/95	JP 7193569 A		28/07/95
		US 5371794 A		06/12/94
EP 0447380 B1	18/09/91	AT 121254 T		15/04/95
		AU 638820 B		08/07/93
		AU 7495291 A		10/10/91
		CA 2051385 A		10/09/91
		CN 1024241 B		13/04/94
		CN 1054868 A		25/09/91
		DE 69008167 D,T		22/09/94
		DE 69108762 D,T		24/08/95
		EP 0460181 A,B		11/12/91
		ES 2073726 T		16/08/95
		HK 101895 A		30/06/95
		IE 67887 B		01/05/96
		JP 4505693 T		01/10/92
		NO 300249 B		28/04/97
		PT 96979 A		30/04/93
		SE 465800 B,C		28/10/91
		SE 9000856 A		10/09/91
		US 5282250 A		25/01/94
		US 5390245 A		14/02/95
		US 5559886 A		24/09/96
		WO 9114348 A		19/09/91
WO 9114348 A1	19/09/91	AT 121254 T		15/04/95
		AU 638820 B		08/07/93
		AU 7495291 A		10/10/91
		CA 2051385 A		10/09/91
		CN 1024241 B		13/04/94
		CN 1054868 A		25/09/91
		DE 69008167 D,T		22/09/94
		DE 69108762 D,T		24/08/95
		EP 0447380 A,B		18/09/91
		EP 0460181 A,B		11/12/91
		ES 2073726 T		16/08/95
		HK 101895 A		30/06/95
		IE 67887 B		01/05/96
		JP 4505693 T		01/10/92
		NO 300249 B		28/04/97
		PT 96979 A		30/04/93
		SE 465800 B,C		28/10/91
		SE 9000856 A		10/09/91
		US 5282250 A		25/01/94
		US 5390245 A		14/02/95
		US 5559886 A		24/09/96
US 5345506 A	06/09/94	JP 5344117 A		24/12/93

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAHPS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.